End User Control Panel
(EUCP)

User Guide

INTRODUCTION…….……3

Setting Up Your Internet Service……...3

Basic Requirements……3

END USER CONTROL PANEL……...4

EUCP – Change Personal Info……...5

EUCP – Change Password…….5

EUCP – Modify Spam and Virus Settings…….6

EUCP – Advanced Spam Settings and Filtering Options……..9

EUCP – Manage Website……...…..12

EUCP – Webmail…….…..…..14

EUCP – Greymail……...…..…….15

EUCP – Content Filtering/Parental Controls/Tattle-mail…….16

EUCP – E-mail Settings…….……...19

EUCP – N-Drive Remote Network Storage…….20

ADDITIONAL RESOURCES…….24

Video E-mail and Userid and Password Attributes……..……24

Introduction

This document is a user manual for your e-mail and Internet services. It provides instructions for managing your e-mail account(s) with the End User Control Panel, including personal information and password changes, spam and virus settings, Webmail (e-mail access from the World Wide Web), Greymail (spam and virus repository), Content Filtering and Parental Controls. It also covers features like Roaming Access, Personal and Corporate Web Space, Video e-mail, and other services. SkyBest reserves the right to make these controls available to you or manage these controls on your behalf. Therefore, you may or may not have access to the controls mentioned in this manual. Screen shots used in this manual are for examples only. Your actual screens may vary depending upon the controls and services made available to you by SkyBest. Contact SkyBest Customer Service if you have questions regarding controls and services that are available to you.

Setting Up your Internet Service

SkyBest has several options for establishing your e-mail and Internet service. Contact SkyBest Customer Service if you have questions related to the initial setup of your account. This manual is intended to cover managing your account and services after your account(s) are established.

Basic Requirements

Userid's and Passwords

Userid's should be entered in all lower case letters, since many e-mail systems can only accept e-mail addresses in lower case and your userid is an e-mail address in this system. However, passwords are case sensitive, meaning upper or lower case letters used to establish your password will be checked for matching case each time you log in. This provides an increased level of security with less likelihood of your account(s) being accessed by password generation technology employed by hackers and identity thieves. Users must log in with their full userid **(bobsmith@skybest.com for example)** and password when initiating e-mail sessions in order to be able to send e-mail as detailed below. Please guard your userid and password information carefully. See the Additional Resources section for password attributes, length, legal characters, etc.

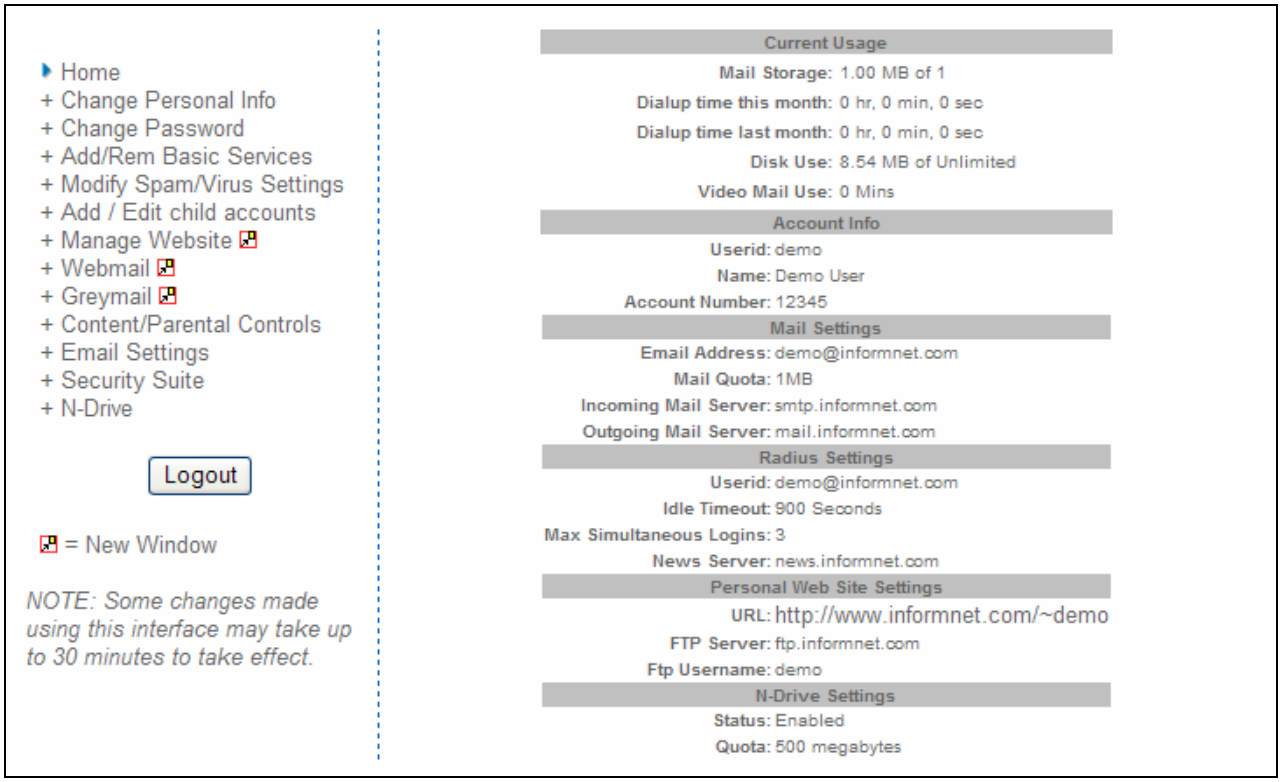
SMTP Authentication

In order to reduce virus and spam proliferation, the outgoing e-mail servers used to support your e-mail account(s) require SMTP Authentication. This will require that minor configuration changes in your e-mail program be updated to support and enable SMTP Authentication, and that you log in with your full userid and password when initiating an e-mail session. Otherwise, you will not be authorized to send e-mail and will receive error notifications upon attempting to send e-mail. This is an important step in preventing unauthorized individuals from distributing attacks and junk e-mail, and in uniquely identifying those users who launch such attacks. This support only has to be enabled once for each account.

End User Control Panel

The End User Control Panel (EUCP) is a quick and easy way for you to manage your Internet account and account settings via the web.

To access the EUCP, you must browse to http://myaccount.skybest.com. Once there, you must enter your full userid and password to log in. You will then see the home page below which shows your current usage for the month (metered Dialup), your account information, as well as your mail, radius, and personal website settings. This is a good location to check your e-mail and personal web storage info. This screen is known as: Home in the drop down menu on the left.

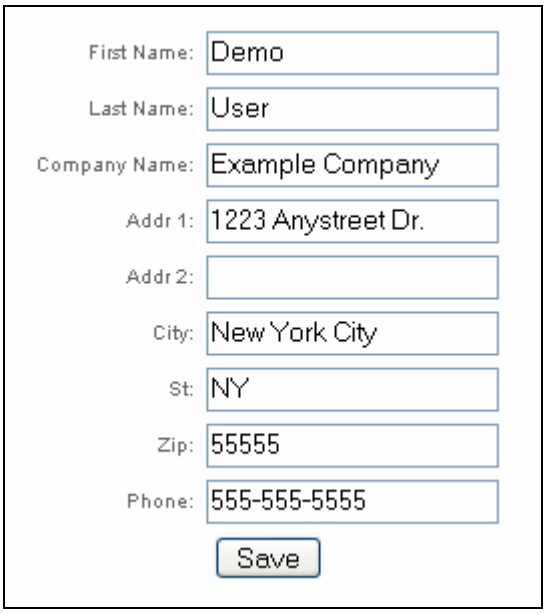


Please take a look at the menu on the left side of the main page above. This menu gives you the ability to make changes to the services you receive. You can make changes to the services listed in the menu above and below you will find instructions on each one. As noted, some changes made using this interface may take up to 30 minutes to take effect.

As mentioned earlier, you may not have the ability to change all of these services shown. The parameters shown in the account info on the right are for example only and may not reflect the settings of your actual account. Some screens in this manual may not appear like actual screens.

EUCP - Change Personal Info

By clicking on this link, the screen below allows you to update your personal information. Customer Service will be notified of the changes you are making within 24 hours. Remember to click on **Save** after you have entered in your new information!



EUCP - Change Password

The screen shown below allows you to change your password. Remember that passwords are case sensitive. You must input your existing password and then a new password; you will then need to verify your new password. This will ensure that you do not mistype the new password. Remember to click on **Save** after you have entered in your new information! It is important to remember that it could take up to 30 minutes after you click **Save** for this change to take effect, and it will affect all services that require you to login with userid and password.

Forgot your password? Contact SkyBest Customer Service.

See the Additional Resources section for password attributes, length, legal characters, etc.

EUCP - Modify Spam and Virus Settings

With anti-spam and anti-virus services your time spent using the Internet is now much more enjoyable! Your e-mails that are classified as spam and those containing viruses are quarantined in one location for you which is called "Greymail", so your inbox isn't cluttered with spam and your computer and valuable data aren't at risk of being corrupted by dangerous viruses. If you have a Tattle-mail password in place, this link will not appear on your EUCP. With a Tattle-mail password in place, only the Greymail OPTIONS link can be used to access these changes. See the section on Content Filtering and Parental Controls for a description of the Tattle-mail feature.

If your anti-spam and anti-virus services are not automatically set up for you, you may set them up by visiting the End User Control Panel, and logging in to enable your service and manage your settings. There is also a link to Greymail from the End User Control Panel for your convenience, and the **OPTIONS** tab in Greymail can also be used to adjust your spam and virus filtering options.

Once you have logged in to the EUCP with your userid and password, click on **Modify Spam/Virus Settings** on the left-hand menu. You will then see the following items which you are allowed to modify. A brief explanation of each item is provided below:

E-mail messages categorized as spam are left in your Greymail for 14 days as the default setting. You are allowed to change this period of time. You can leave a message in Greymail for any amount of time between 1 and 14 days. It is recommended to not set this time period too low so that you will have enough time to retrieve any e-mail from Greymail that you would actually like to receive. Log in to Greymail, check the box beside the message(s) you would like to receive and click forward. Selected messages are then forwarded to your inbox. Set the amount of days you want messages to remain in your Greymail and then select **Change**. You cannot forward e-mails that contain viruses to your inbox.

You have the ability to turn your Spam Filtering service off by selecting the **Off** tab**.** If you choose to employ Content Filtering, then you can select the **Content-Based** tab for Content-Based filtering and then clicking **Change**. Spam Filtering options will be detailed later in this document.

A Greymail Notification consists of an e-mailed report containing all of the e-mails you received which were either classified as spam or classified as containing a virus and were sent to your Greymail. You can decide to receive this report on a daily or weekly basis or not to receive it at all by clicking on one of the options below and then clicking on **Change**.

The Virus Filtering Section simply allows you to turn on or off your Virus Filtering service. This action may be recommended when you use additional software to provide virus protection. (SkyBest may elect to have this function on at all times regardless of the user settings to prevent proliferation of viruses.)

The Virus Notification is an e-mail which is sent to you and the e-mail sender each time an e-mail is flagged as containing a virus. You have the ability to turn this service on or off as shown below.

By selecting **Content-Based Spam Filtering** option, you then have the ability to enter Advanced Spam Settings, create a Blacklist, a Whitelist, and direct mail from blacklisted senders to Discard or Graymail. (See details below). Otherwise, these options do not appear on the EUCP.

Advanced Spam Settings is the section you would use to edit your spam sensitivity settings and specify types of spam to quarantine to Greymail. By selecting **Edit** here you will then be able to modify your settings. The Advanced Spam Settings will be detailed later in this document.

The Blacklist is a mechanism for blocking e-mails from specific e-mail addresses. If you do not want to receive e-mails from certain senders you may add their addresses in this section.

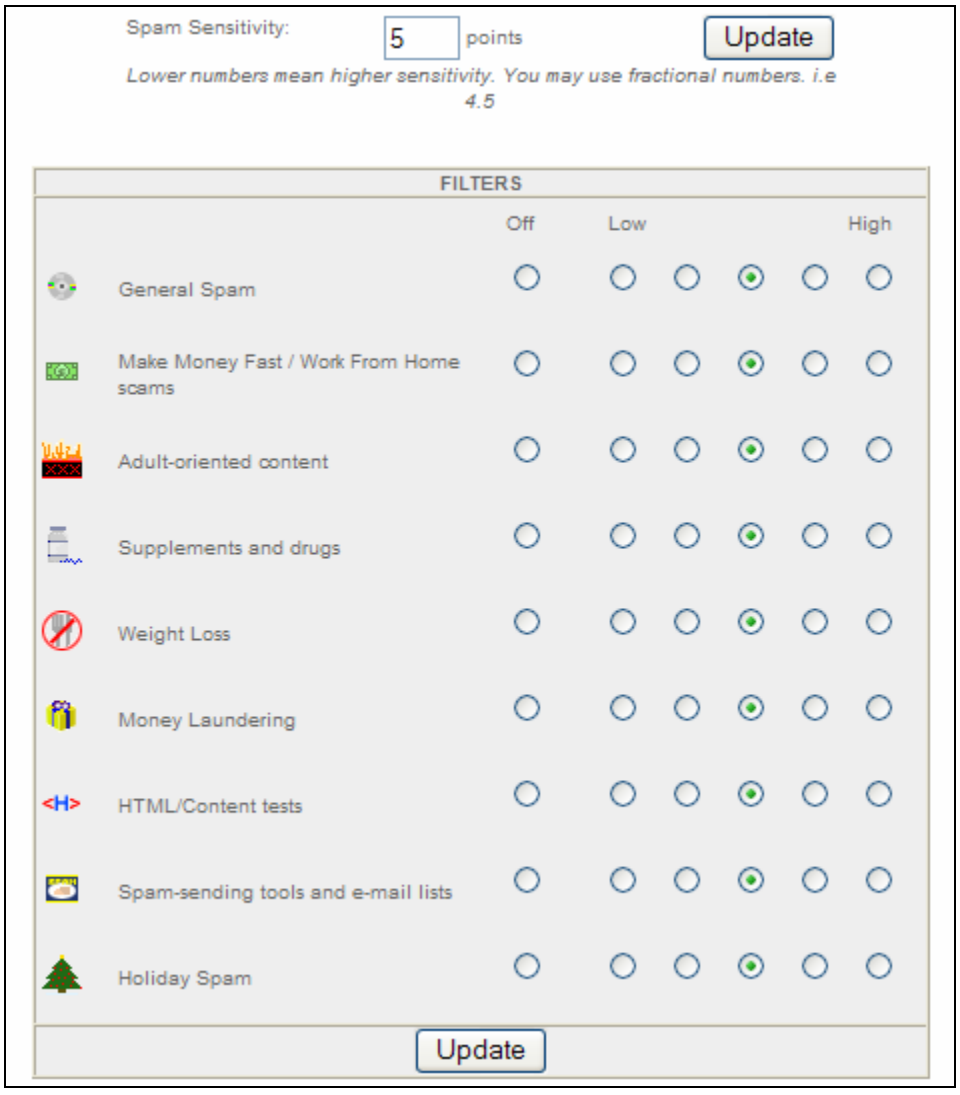
The Whitelist allows you to make sure that you always receive e-mails from specific senders. To ensure that a certain someone's e-mails are not sent to Greymail, add them to this list.

Both the Blacklist and Whitelist functions will accept "wildcards" using an asterisk "*" as the wildcard. Using wildcards in front of a portion of an e-mail address means every address that matches the rest of the address will be affected. For instance, if you were to put the following address in your Blacklist file: "*@bobdomain.net", then all mail from anyone in the "bobdomain.net" domain would be sent to Greymail. Similarly, if you were to put the following address in your Whitelist file: "*@joedomain.net", then all mail from anyone in the "joedomain.net" domain would be sent to your inbox, provided no viruses were detected.

Finally, you also have the option of having e-mail sent from a Blacklisted sender either discarded immediately, in which case you will never know it was sent to you, or you can choose to have it sent to your Greymail. The default setting is Greymail, and is recommended.

EUCP - Advanced Spam Settings and Filtering Options

By selecting **Edit** on the Advanced Spam Settings section under Modify Spam/Virus settings, you will then be able to modify your settings. Advanced Spam Settings and Filtering adjustments allow you to customize your spam filters based upon the content within specific e-mails. Use these screens to edit your spam sensitivity settings and adjust filters for specific types of spam.

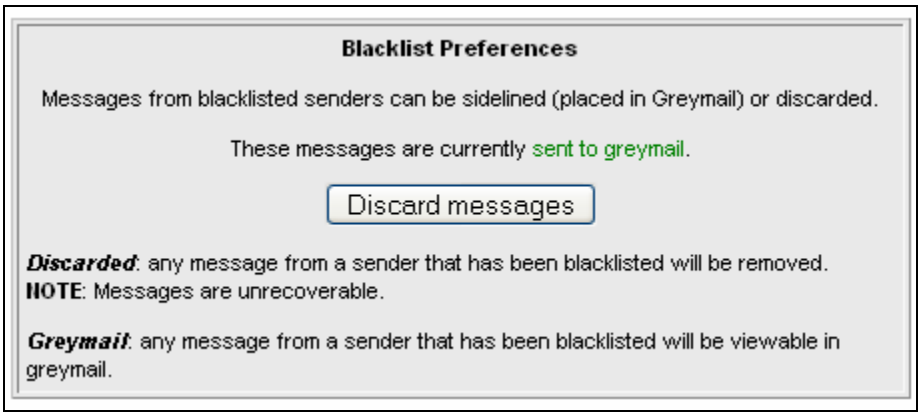


You have the ability to set an overall Spam Filtering sensitivity above. You can set sensitivity anywhere between 0 and 999, where the lowest number indicates the strongest of filtering settings. The default setting is 5. You can also choose the level for each individual filter. Experiment with the filters until you are satisfied with your exact filtering specifications. After making your changes, select **Update** in order for your settings to take effect. Below this panel you will see the Real Time Block list panel described on the next page.

Real Time Blocks are a method of blocking e-mails from specific countries that originate spam. Once you make changes, you must click **Update** so that your new selections go into effect. It is recommended to leave **RBL** and **Dialup List** checked, as these are lists of addresses known to generate spam. You can also **Edit** and **Save** your Blacklist and Whitelist settings as shown below.

REALTIME BLOCKS
Block mail from Argentina
Block mail from Belgium
Block mail from Brazil
Block mail from China
Block mail from Colombia
Block mail from Germany
Block mail from Greece
Block mail from Hong Kong
Block mail from India
Block mail from Italy
Block mail from Japan
Block mail from Korea
Block mail from Kuwait
Block mail from Malaysia
Block mail from Mexico
Block mail from Nigeria
Block mail from Peru
Block mail from Philippines
Block mail from Russia
Block mail from Singapore
Block mail from Spain
Block mail from Taiwan
Block mail from Thailand
Block mail from Turkey
Block mail from United Kingdom
Dial Up List
RBL
Update
Blacklist
Add or edit names in the list, then hit save.
All mail coming from these senders will be blocked.
Save
Whitelist
Add or edit names in the list, then hit save.
Spam Mail coming from these senders will not be blocked.
Viruses coming from these senders will always be blocked.
Save

The screens below are used to select your Blacklist actions, Spam Life, Virus Notification, and Greymail Notification settings as described earlier in this document.

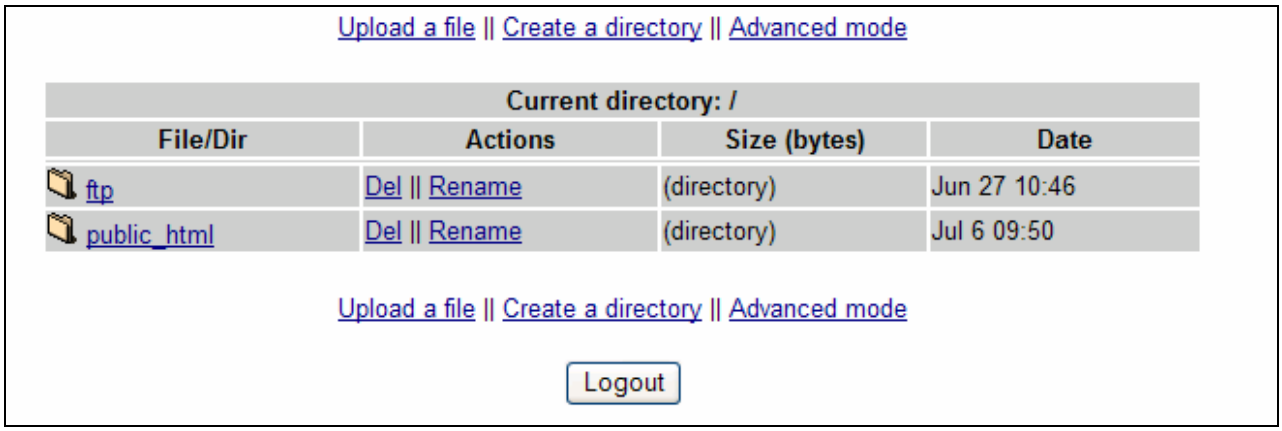

Blacklist Preferences
Messages from blacklisted senders can be sidelined (placed in Greymail) or discarded.
These messages are currently sent to greymail.
Discard messages
Discarded: any message from a sender that has been blacklisted will be removed.
NOTE: Messages are unrecoverable.
Greymail: any message from a sender that has been blacklisted will be viewable in greymail.

Spam Life
Spam and Virus messages are automatically purged from greymail.
You can select the number of days a message stays in the mailbox.
This can be between 1 and 14 days.
Automatically delete messages after
5
days.
Change

Virus Notification
Greymail can automatically send you an email when you receive a message containing a virus.
This feature is presently Off.
Turn notification on

EUCP - Manage Website

The **Manage Website** link will take you to the control panel shown below. Personal web space is a repository for you to store a website, documents, images, files or photos. This space is "write" accessible by you, the site owner, by using your Internet browser, Web Page Editor, or ftp (File Transfer Protocol) Application. It is also "read" accessible to the rest of the world by typing the web space URL (Uniform Resource Locator, also known as your web address) into their Internet browser. Your web space administration is password protected so your files will stay safe and secure and will only be available for others to view or copy by surfing to your URL.



How do I put files into my web space?

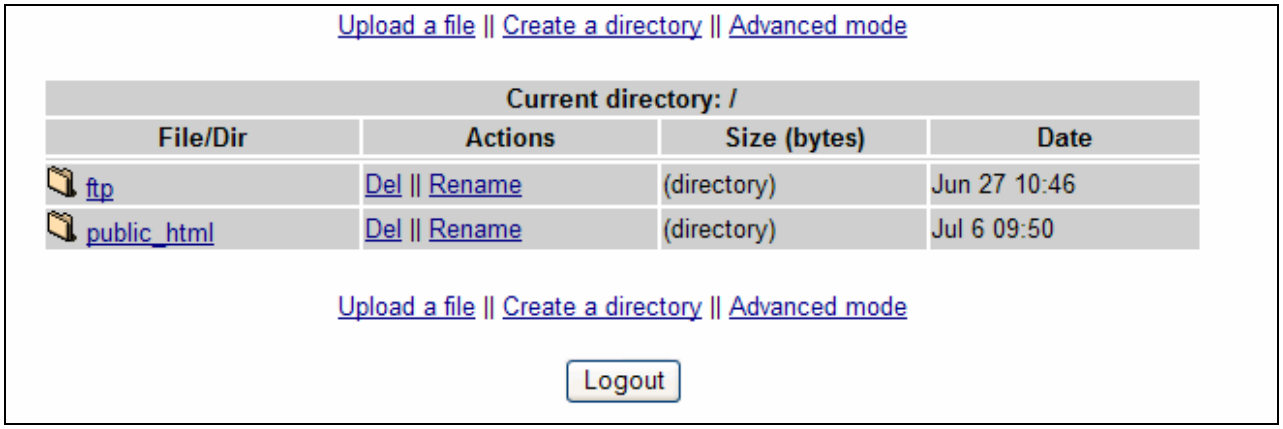
In order for files to become available from your personal web space, you must first put them there. The method of doing this is called "File Transfer Protocol" (ftp). FTP is the method of delivery, but you must have a way to use this method known as an ftp client. An ftp client is a software application that allows you to put files on the server (upload), and get files from the server (download). There are several types of clients that can be used, as mentioned below. When you select **Manage Website**, you see the one above.

What clients can I use to put files in my web space?

As mentioned before, there are several types of ftp clients. Programs such as "WsFTP" and "SmartFTP" are 100% ftp clients. This means that their only function is to put files on a server and get files from a server. These are great for people who are only storing files in their web space or are using a text editor (like Notepad or WordPad) to create web pages and then uploading them when they are done. Programs like "Dream Weaver" and "FrontPage" are webpage editors (also known as HTML editors) that, in addition to creating and editing web pages, also have a built-in ftp client. This is handy for creating many web pages and then uploading them quickly. And lastly, there is the web based software that you access from the **Manage Website** link. Our ftp tool allows you to upload files from your Internet browser without the need for these third-party programs. Simply go to our ftp site, log in with your userid and password, choose the directory that you would like to put your files in and then upload. See details below:

What steps do I take to use the web-based ftp tool?

1. Surf to http://webftp.skybest.com
2. Enter your userid and password.
3. Click the link of the folder you want to upload your files



The "public_html" folder is where you would place all of your webpage related files and images. "Username" is the portion of your e-mail address in front of the @symbol, for instance bob@skybest.com would have a username of "bob".

This public_html folder is accessible to the rest of the world by surfing to http://www.skybest.com/~username (be sure to put a "~" in front of your username.)

The ftp folder is accessible by anonymous ftp, which means a user can surf to ftp://ftp.skybest.com/username. (No Tilde ~ needed)

Once you are inside your desired folder, you are presented with three options:

- **Upload A File**: Allows you to put a file from your computer to your web space.
- **Create A Directory**: Organize your web space by creating additional folders.
- **Advanced Mode**: View important information about your files and change permissions.

What are the addresses that I give to friends and family?

All addresses are composed of two things, the domain of your ISP and your userid.

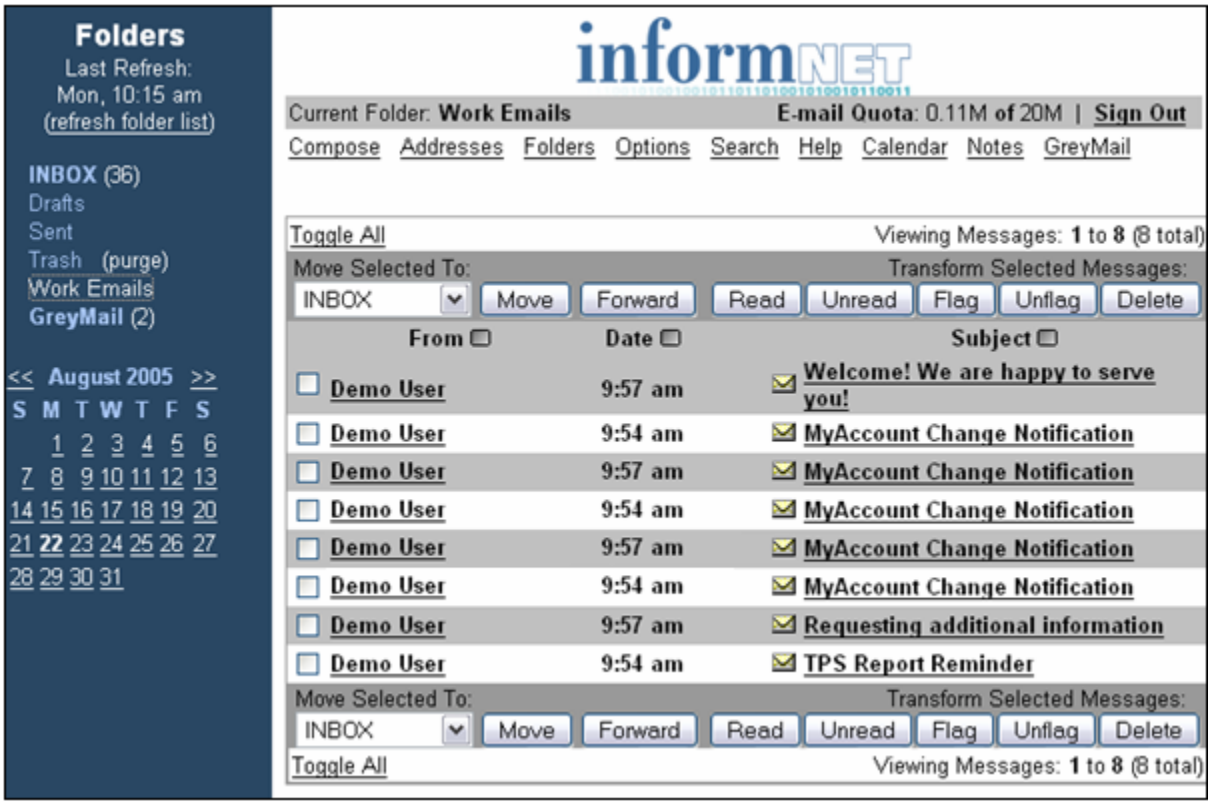
Listed below is the format you would use to access these "sites".

- I want to access my files directly from an Internet Browser using ftp:
  - ftp://ftp.skybest.com/username (no Tilde ~)
- I want my friends/family to see my webpage:
  - http://www.skybest.com/~username
- I made a folder called "images" in my public_html directory, how do I access it:
  - http://www.skybest.com/~username/images

EUCP - Webmail

The **Webmail** link on the EUCP takes you to your Webmail account. You can also access your Webmail account by browsing to http://webmail.skybest.com and logging in with your full userid (e-mail address) and password.

Webmail allows users to access their e-mail from the Web. They can create and send new messages, import or create contact lists, reply to or forward e-mail, or set up folders to file and store e-mail on the server. They can use the personal calendar, create notes and reminders, or access Greymail to check quarantined spam e-mails or e-mails containing viruses from the Greymail link. For more information on using Webmail, see the built in Help files.



EUCP - Greymail

This link on the EUCP takes you to your Greymail account, where you will find e-mails determined to be spam and e-mails containing viruses. You may also access Greymail by browsing to
http://greymail.skybest.com. The Greymail home page is shown below.

Please note the **OPTIONS** link at the top right of the Greymail home page above. When you click on this link, you will see the advanced spam settings detailed in the Advanced Spam Settings section shown earlier in this manual.

Please note the icons at the top right of the Greymail home page which are shown below.
:

Tag messages by selecting the **tag box** to the left of the message. You can tag **All** or **None** using these boxes in the header. Selecting the icons above will then take actions as described below.

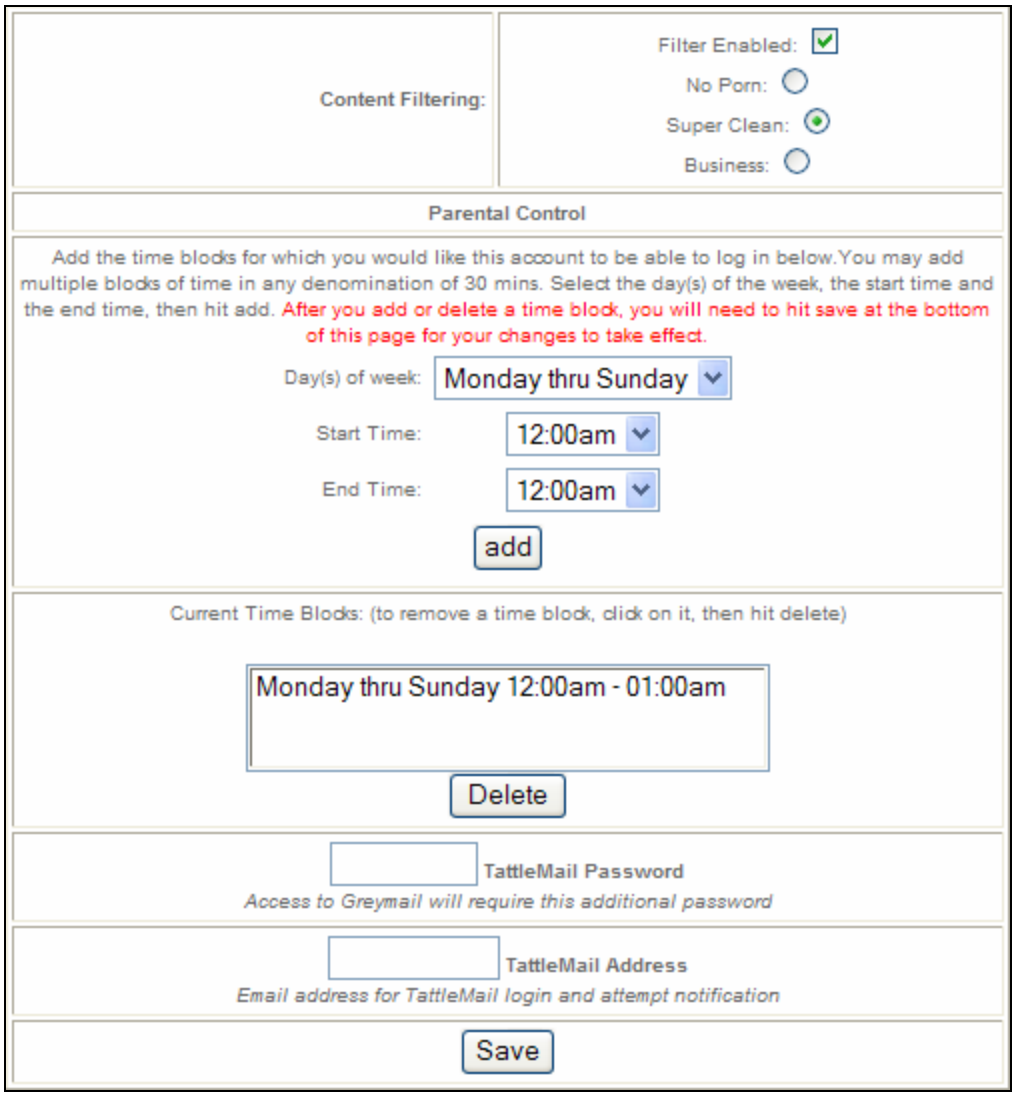
- **Mark as Read** - You have the ability to tag an e-mail (click on the box to the left of the e-mail and you will see a checkmark appear) and then click the **Mark as Read** icon and that e-mail will now show that it has been read.
- **Mark as Unread** - You have the ability to tag an e-mail and then click the **Mark as Unread** icon and that e-mail will now show that it has never been opened.
- **Delete Selected** - This icon allows you to delete e-mails you have tagged.
- **Forward Selected** – Check the box to the left of any e-mail you would like forwarded to your inbox then click this icon. The e-mail will be forwarded to your inbox.
- **Forward and Allow** – This icon forwards the selected e-mail(s) to your inbox and places the sender's e-mail address on your Whitelist. You will be taken to the Greymail options page and must select the **Save** button under your Whitelist to save your changes.

- **Allow Sender** - If you tag an e-mail in your Greymail and then click on the **Allow Sender** icon, this e-mail address will be placed on your Whitelist. You will be taken to the Greymail options page and must select the **Save** button under your Whitelist to save your changes.
- **View Stats** - By clicking on the **View Stats** icon, you will be able to view your spam and virus statistics for the months you have had service.

EUCP - Content Filtering/Parental Controls/Tattle-mail

This section of the EUCP allows you to manage your Content Filtering, Parental Controls and Tattle-mail. See below for descriptions of the options available on this screen.

(Note: Content Filtering and Parental Controls, and may not be available to all users. These features require specific authentication methods in order to perform their function. Contact your service provider for further information.)


Content Filtering:
Filter Enabled:
No Porn:
Super Clean:
Business:
Parental Control
Add the time blocks for which you would like this account to be able to log in below.You may add multiple blocks of time in any denomination of 30 mins. Select the day(s) of the week, the start time and the end time, then hit add. After you add or delete a time block, you will need to hit save at the bottom of this page for your changes to take effect.
Day(s) of week:
Monday thru Sunday
Start Time:
12:00am
End Time:
12:00am
add
Current Time Blocks: (to remove a time block, click on it, then hit delete)
Monday thru Sunday 12:00am - 01:00am
Delete
TattleMail Password
Access to Greymail will require this additional password
TattleMail Address
Email address for TattleMail login and attempt notification
Save

In the screen shot above, you have the option to enable Content Filtering and choose which level of filtering you want. Your three choices are described below. You will not notice that Content Filtering is in effect until you try to reach a site that has been deemed unacceptable, in which case you will see an "Access Denied" screen similar to the one below.

Access Denied
We are sorry, but the site or resource you are trying to access has been blocked by your Internet Service Provider.
If you feel that this access denial is an error, please contact your Internet Service Provider to correct this issue.

If enabled, the content filter automatically activates upon logging in, using the selected filter:

- **No Porn:**
  No public proxies or pornography sites are allowed to be accessed.
- **Super Clean:**
  No alcohol, Anarchy, Criminal Skills, Cults, Drugs, Gambling, Hate Groups, Obscene & Tasteless, Public Proxies, Pornography, or R-Rated sites are allowed to be accessed.
- **Business:**
  No Alcohol, Anarchy, Chat, Criminal Skills, Drugs, Employment, Financial, Gambling, Games, Hate Groups, Humor, Obscene & Tasteless, Public Proxies, Personals, Pornography, R- Rated, Shopping, Sports, Web Based E-mail, Web Based Newsgroups.

Once you have made your selections, you must click **Save** and your requests will be made within 30 minutes. You must logoff and re-enter the system for these changes to take effect, or they will take effect the next time you log in.

Under the section labeled "Parental Controls" above, you can add and delete time blocks for which you want an account to be able to access the Internet. You simply select the day(s) of the week, the start time and the end time, then hit **Add**. You will see your changes go into effect within 30 minutes. Again, you must logoff and re-enter the system for these changes to take effect, or they will take effect the next time you log in. (No entry allows access at any time.)

Password and an e-mail address are options for Tattle-mail on the screen shot above. Tattle-mail is a mechanism that allows parents to be notified if their children or someone using one of their child accounts is trying to access the contents of Greymail. Oftentimes, the nature of the spam e-mails in your Greymail can be unsuitable for children, and by providing an e-mail address and password for Tattle-mail, you will be able to make sure your children don't access Greymail and if they try, you will be notified via e-mail to the address you specify. See Modify Spam and Virus Settings

EUCP - E-mail Settings

In the E-mail Settings section you may have the ability to set-up e-mail aliases and to set-up e-mail forwards. SkyBest reserves the right to make these controls available to you or manage these controls on your behalf.

Upon clicking on the **E-mail Settings** link, you will see a screen like the one below:

The E-mail Alias section above allows you to add up to 100 different addresses for which e-mail arrives at your one main account. For example, if your userid is “Bob” and you make an alias called “Jim”, any mail sent to “Jim@domain.com” will be delivered to your “Bob@domain.com” account. You must click on **Save** to save your changes to this panel.

In the section labeled “Forward all mail to:” above, you can insert a new address for which you would like all e-mail addressed to your old address to be forwarded to. Your existing mail will be removed from the mail server, and all new mail will be redirected to the e-mail address that you enter. It is very important to retrieve any existing mail from the server before you enable this feature or it will be lost permanently. To remove a forwarder, simply delete it, then click on **Save**.

EUCP - N-Drive Remote Network Storage

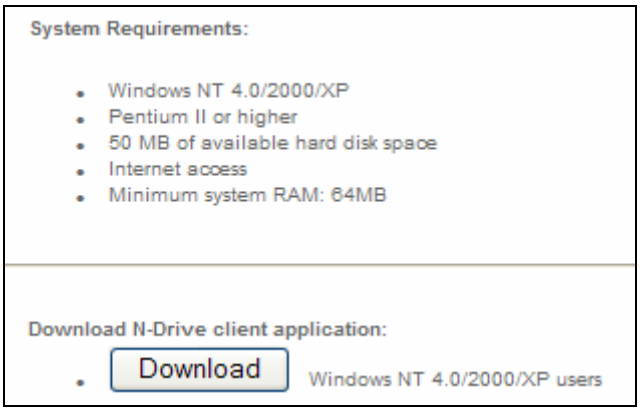
Storing critical files on the network reduces the risk or impact of malicious attacks, viruses, hardware problems, accidental deletion and lost or damaged equipment. N-Drive Remote Network Storage provides a safe and secure storage facility on a network server for storing text documents, photos, web pages, spreadsheets and other files. N-Drive combines the security of network storage with the convenience of a local drive. Once N-Drive is enabled, the network drive is accessible from within applications just like a local drive on your computer.

You can drag and drop or copy files to or from the network drive server using Windows Explorer or using DOS commands or Save/Save-as commands within many applications. Searches can also be extended to network drives. Backups can be scheduled and run automatically using the File Transfer Manager, and full or incremental backups are supported. N-Drive makes using remote storage quick, easy, and reliable.

N-Drive allows users with Windows NT 4.0/2000 & XP Operating Systems to securely transfer, store and access files, without having to learn a new application. FTPS using Secure Sockets Layer (SSL) is supported by N-Drive by creating an encrypted "tunnel" through which FTP transfers data. Secure FTP or SFTP is also supported by N-Drive and provides 128-bit encryption of all transmitted data. Server side support is required for both of these secure protocols.

Downloading the N-Drive Client

Selecting the **N-Drive** link on the End User Control Panel will display the System Requirements/Download page shown below. Selecting the **Download** link will begin the download process. Versions of Windows Operating systems not shown on the System Requirements page will not work with N-Drive. It is recommended that you upgrade to a supported Operating System in order to use this product. It is necessary to contact Customer Service to activate this product. Be sure and ask about a number of storage capacities that are available. This product may incur additional billing when used.



Installing the N-Drive Client

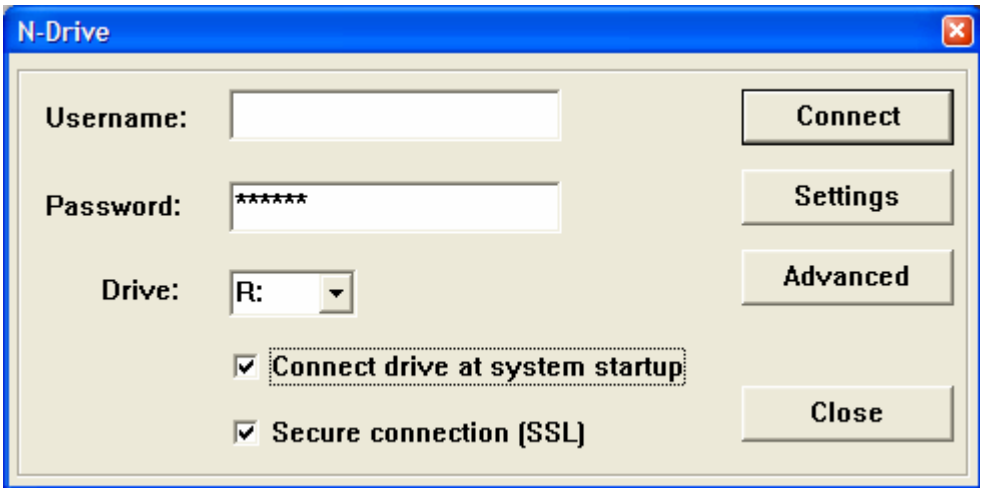
After selecting the **download** box, you will be asked if you want to run or save the installer application. Select **Run** or **Save.** If **Run** is selected, the installer will begin and open the Install Wizard. If **Save** is selected, the installer file will be downloaded to the location specified in the **Save As** dialog box. Once saved, locate the installer application and double click on it to begin the install process. The installer application is typically named setupXYZ.exe, where XYZ refers to the version of the Windows Operating system supported by the installer.

The Install Wizard will prompt you for the folder destination to install the N-Drive program files. You can browse to select the folder for the installation and then click on **Next** to install or click on **Cancel** to exit the Install Wizard. The Install Wizard will copy the program files to the destination folder and then install the program. A restart is required to activate the N-Drive application.

The Install Wizard will also create shortcuts in the Start Menu\All Programs\N-Drive folder for N-Drive and Uninstall N-Drive. Select the shortcut to run the program. The Uninstall shortcut is used to uninstall the program, should this be required.

Starting N-Drive

When the N-Drive program is initiated for the first time by selecting the program icon in the Start Menu Programs list, system tray, or double clicking the shortcut, the following screen is shown: (Your Userid will be displayed in the Username field.)



This screen serves several functions including as detailed below:

- Allow access to network storage functionality through your full e-mail username and password. (This functionality must be activated by Customer Service.)
- Selecting the Drive letter associated with the network drive from the drop down menu (Typically, letters D thru Z can be assigned as the drive designator.)

- Selecting whether you want the drive to connect at system startup by clicking on this checkbox. This will connect the drive each time your system starts or restarts.

- Select whether you want SSL (Secure Sockets Layer) protocol used in file transfers by clicking on this checkbox (SSL availability requires Windows NT 4.0/2000/XP)

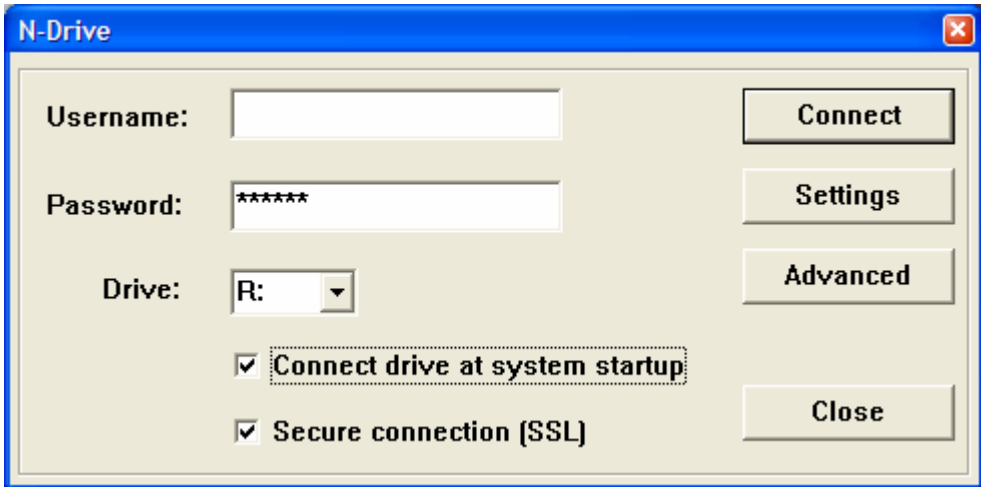
- Access to General settings for the network storage application by clicking on the **Settings** tab (It is recommended to leave these settings at their default values.)

- Access to Advanced settings for the network storage application by clicking on the **Advanced** tab (It is recommended to leave these settings at their default values.)

- When the username, password, and drive letter selections are complete, and choices are made for Connection at startup, SSL encryption, General, and Advanced Settings, click on **Connect** to connect the network drive and finish the initiation of the program.

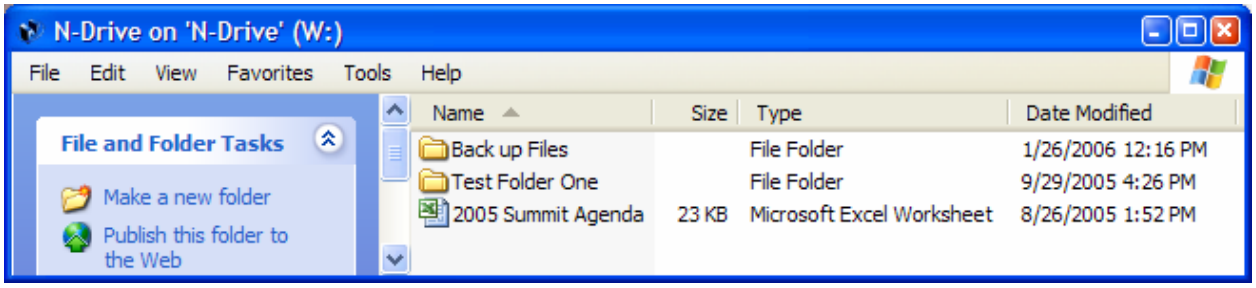
Using N-Drive

Once the program is initiated, a screen will be displayed showing the network drive with its designator is connected and available for use just like any other drive on the computer.

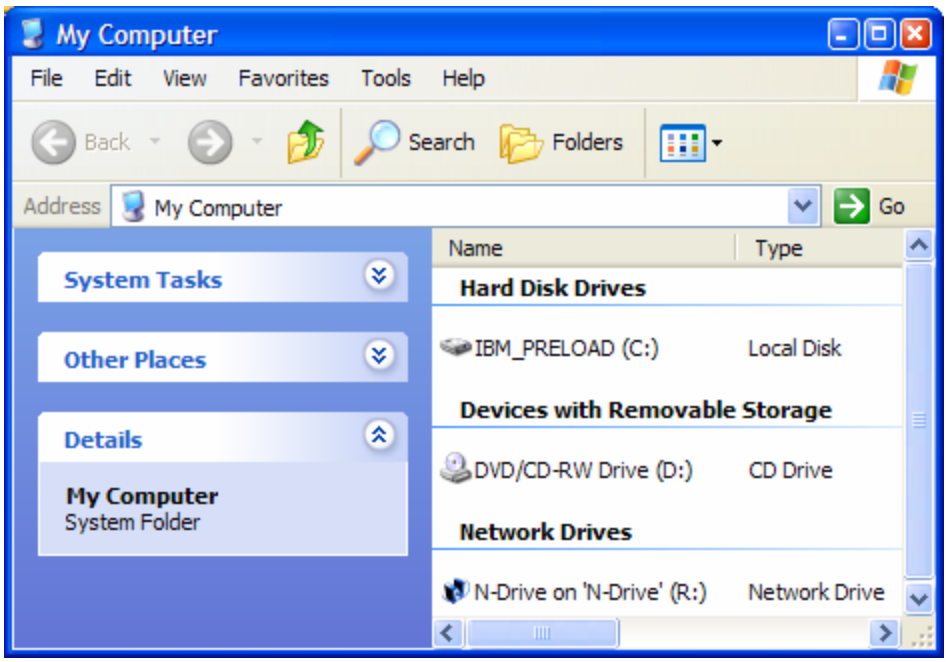


If users elect not to have the network drive connect on system start-up, they can connect the drive by selecting the **Start Menu, All Programs**, and the **N-Drive** program icon from the program list to connect the drive. The same starting network storage connection screen above will appear. The username and password will already be populated and should not be re-input unless a change is required (Your Userid will be displayed in the Username field.) The same selections are available for Connection at startup, SSL encryption, General, and Advanced settings. Click on **Connect** to connect the drive.

The network drive will appear in most Windows applications when users select a **Save As** function and can be chosen as the target drive for saving files or creating folders. The network drive is available for file and directory manipulation using DOS commands. The network drive is also available for most search applications and will display folders or files matching the search criteria.



The network drive will appear when the user selects **My Computer** to display other hard disk drives and devices with removable storage (Hard Drive/CD/DVD/Floppy drives**). Files and folders can be "dragged and dropped" onto the drive icon to create copies of these files and folders on the network drive.



** Note: (100GB free space for network storage is shown incorrectly in these screens and is a function of how the Windows Operating System interacts with network drives. Actual capacity will be determined by the network storage package/offering.

We hope you find this to be a safe, secure and convenient method of using network storage to reduce the risk of lost, deleted or damaged information.

Additional Resources

Log in to www.skybest.com for further information regarding your e-mail and Internet services.

You can contact our Customer Service department at 1-800-759-2226.

For technical support questions regarding your e-mail or Internet services, contact our Technical Support/Help Desk at 1-866-759-7591.

Video E-mail

A new feature included with the new platform is video e-mail. If you have a webcam and a microphone, video e-mail allows you to record video and audio and then include a link in your e-mail message that will allow the receiver to access a server to view and hear the recorded message. There is no special software needed, and video e-mail does not include a large attachment--only a link to the files. Video e-mail can only be used via the Webmail link.

Userid and Password Attributes

The following attributes represent the acceptable parameters for Userid's and passwords.

Userid's

Userid's must be **at least 2, but not more than 20 characters in length**. **(No spaces)**
Userid's may only contain the following characters:
Letters A thru Z,
Digits 0-9
Underscore (_)
Dash (-)
Period or Dot (.),
Userid's may not begin or end with dot, dash or underscore.

Upper and lower case Userid's will be accepted, but any uppercase characters will converted to lowercase automatically. Many e-mail systems only accept lower case e-mail addresses or convert them to lower case. (Since our systems use the e-mail address as the userid, this convention ensures that Bob@skybest.com and bob@skybest.com do not get each others e-mail.)

Passwords

Passwords must be at least 2 but no more than 16 charters in length. (No spaces)
Passwords are case sensitive. Case matching will be enforced for passwords.
Passwords may only contain the following characters:
Letters A thru Z,
Digits 0-9
Underscore (_)
Dash (-)
Period or Dot (.),
Passwords may not begin or end with dot, dash or underscore.